



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/613,125	07/07/2003	Kyung-Hun Jang	249/387	7220
27849	7590	07/07/2008		
LEE & MORSE, P.C. 3141 FAIRVIEW PARK DRIVE SUITE 500 FALLS CHURCH, VA 22042			EXAMINER SHAN, APRIL YING	
			ART UNIT 2135	PAPER NUMBER
			MAIL DATE 07/07/2008	DELIVERY MODE PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

10/613,125

Applicant(s)

JANG ET AL.

Examiner

APRIL Y. SHAN

Art Unit

2135

Period for Reply -- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 22 May 2008 and 04 April 2008.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-5, 7-18 and 20-25 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-5, 7-18 and 20-25 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/SB08)
Paper No(s)/Mail Date _____
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date _____
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: _____

DETAILED ACTION

1. A Request for Continued Examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 4 April 2008 and 22 May 2008 (preliminary amendment) has been entered.
2. Claims 1, 3, 5, 7-8, 12, 14, 16-18 and 20-25 have been amended. Claims 6 and 19 have been canceled. No new claims have been added. Claims 1-5, 7-18 and 20-25 are currently pending in the present application.
3. Applicant's amendments and argument have been respectfully and fully considered, but are moot in view of new ground rejection as set forth below.
4. Any rejection/objection not repeated below is withdrawn to due to Applicant's amendment.

Claim Objections

5. Claims 23-25 are objected to because of the following informalities:

As per **claim 23**, the amended claim limitation "first means for creating a first group key...communicated using the first group key and a modified second group key, modified according to a predetermined modification time period, communicated using the initial second group key..." is grammatically incomprehensible.

Any claim not specifically addressed, above, is being rejected as incorporating the deficiencies of a claim upon which it depends.

Appropriate correction is required.

Claim Rejections - 35 USC § 112

6. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

7. Claims 1-5, 7-18 and 20-25 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 1 recites the limitation in step (d), "...and transmitting the modified second group key to the (N-1) sub wireless terminals, wherein at least one modified second group key is transmitted and used to encode data during use of the first group key" is being recited. First, it is unclear whether "**the modified second group key**" is intended to be the same as or different from "modifying the initial second group key" as recited in line 1 of step (d) in claim 1. Second, "It is unclear whether "wherein at least one modified second group key" is intended to be the same as or different from the "modifying the initial second group key" recited in line 1 of step (d) in claim 1.

Claim 12 recites the limitation in line 4 of page 5, "...modifies the second group key". It is unclear whether "the second group key" is intended to be the

same as or different from "the initial second group key" recited in lines 2-3 on page 5.

Claim 21 recites the limitation in lines 7-10 of claim 21, "...for transmitting the modified second group key...wherein at least one modified second group key...". First, it is unclear whether "**the modified second group key**" is intended to be the same as or different from "modifying the initial second group key" as recited in lines 6-7 in claim 21. Second, " It is unclear whether "wherein at least one modified second group key" is intended to be the same as or different from the "modifying the initial second group key" recited in lines 6-7 in claim 21.

Claim 23 recites the limitation in line of claim 23, "wherein at least one modified second group key...". It appears to the examiner there are multiple modified second group keys according to this claim limitation. However, from lines 4-7, there is only one modified second group key.

Any claim not specifically addressed, above, is being rejected as incorporating the deficiencies of a claim upon which it depends.

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the

invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

9. The factual inquiries set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 148

USPQ 459 (1966), that are applied for establishing a background for determining

obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

10. This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

11. Claims 1-5, 8-10 and 11-18, 21 and 23-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Asokan et al. ("Key agreement in ad hoc networks", Computer Communications, Volume 23, Number 17, 1 November 2000) in view of Menezes et al. ("Applied Cryptography", pages 551-553, published on October 17, 1996, which is provided by the Applicant).

12. As per **claims 1 and 12**, Asokan et al. discloses a cryptographic method/system using dual keys in a wireless local area network (LAN) system, comprising:

(a) generating a first group key ("At the end of the protocol run, each player shares a key with the leader" - e.g. page 6. Please note a key corresponds to Applicant's first group key) in N wireless terminals (forming an ad-hoc group (an ad-hoc meeting –e.g. p1, "They would like to set up a wireless network session...for the during of the meeting"), where N is equal to or greater than two (P5, "There are two parties A and B which share a weak secret P" and P6 "We can slightly modify this....to a contributory multi-party protocol") ;

(b) generating an initial second group key in a main wireless terminal (a leader – e.g. P6) to perform a key distribution center function among the N wireless terminals in response to a request from one of (N-1) sub wireless terminals ("The leader will broadcast the message in step 1...An additional round will be needed for the leader to pick a common session key and distribute it to the members of the group...he shares with them" – e.g. page 6. Please note on pages 5-6 of Asokan et al. reference, "In step 1 A sends E_a encrypted with the weak secret P...One obvious way to extend this protocol to the multi-party case is to elect a leader", which met the claimed limitation of a request from one of (N-1) sub wireless terminals) the request being communicated using the first group key, and transmitting the initial second group key to (N-1) sub wireless terminals (P6, "An additional round will...to pick a common session key and distribute it the members of the group....he shares with them". Asokan et al. also discloses on page 3, "1.3 Password-based Authenticated Key Exchange...by choosing a fresh password and sharing it among those present in the room...Therefore, we need a protocol to derive a strong shared session key from the weak shared password" – e.g.

page 3. Please note a weak shared password corresponds to Applicant's first group key and a strong shared session key corresponds to Applicant's second group key. Asokan et al. further discloses on page 4, "The basic secrecy requirement is that only those players that know the initial password should learn the resulting session key, which met the claimed limitation of the request being communicated using the first group key. In other words, the requesting member must prove his/her membership in the request by using the initial password (i.e. first group key); and

(c) encoding data using the initial second group key, and transmitting the encoded data between the N wireless terminals (P4 "In a landmark paper [4], Bellovin and Merrit....encrypted key exchange (EKE) and P5 "But the basic form of the generic protocol remains the same." Inherently, Asokan et al. teaches after the protocol is complete, the multi parties must communicate using the session key (the second group key) to encoding data and transmitting the encoded data among the N wireless terminals since the protocol is using encrypted key exchange (EKE), a well known protocol invented by Bellovin and Merrit disclosed on the P4 of the Asokan et al. reference).

(d) modifying the initial second group key in the main wireless terminal according to a modification time period, predetermined in the main wireless terminal, and transmitting the modified second group key to the (N-1) sub wireless terminals, wherein at least one modified second group key is transmitted and used to encode data during use of the first group key (P5, "session key"- a session key is a key that is just used for one communication session and then discarded, Page 20, "multi-

party key agreement will need to address the issues of synchronization and resilience in face of benign faults... and page 11, "at the end of the round, all four players will have the same key...", "The time needed will be the same as that of one two-party key exchange" – page 12, "Synchronous rounds could be implemented if all nodes have loosely synchronized clocks" – page 12, "...key exchange can be done efficiently, in terms of the number of communication rounds.." – page 10, "The protocol proceeds through d rounds, $1, \dots, d$." – page 11 and "...between themselves in $k-1$ rounds...In the end of those $k-1$ rounds each group will have a shared key. For all $2k$ members to agree on a single shared key in round k ...**The time needed will be the same as that of one two-party key exchange.** Notice in round 1 ...In round k ...doing key exchange in parallel" – page 12). Asokan et al. implicitly discloses modifying the initial second group key in the main wireless terminal according to a modification time period, predetermined in the main wireless terminal and transmitting the modified second group key to the $(N-1)$ sub wireless terminals, wherein at least one modified second group key is transmitted and used to encode data during use of the first group key since to an ordinary skill in the art that a session key in the Asokan et al. reference is for a fixed periods (i.e. session) and then need to be replaced and the password (i.e. first group key) is always present to verify membership for broadcasting a new session key the same way as the initial session key (i.e. initial second group key) is transmitted.

In order to make the record clearer, Menezes et al. expressly discloses modifying the initial second group key in the main wireless terminal according to a modification

time period, predetermined in the main wireless terminal ("Cryptoperiods, long-term keys, and short-term keys...The cryptoperiod of a key is the time period over which it is valid for use by legitimate parties...Cryptoperiods may serve to....4. limit the time available for computationally intensive cryptanalytic attacks...short-term keys. These include keys established by key transport or key agreement, and often used as data keys or session keys for a single communication session...**Cryptoperiods limit the use of keys to fixed periods, after which they must be replaced....**13.11

Remark...The term short as used in short-time keys refers to the intended time of the key usage by legitimate parties, rather than the protection lifetime...For example, an encryption key used for only a single session..." – e.g. page 553 of Menezes et al.

It would have been obvious to a person with ordinary skill in the art at the time of the invention to incorporate Menezes et al.'s modifying the initial second group key in the main wireless terminal according to a modification time period, predetermined in the main wireless terminal into Asokan et al.'s motivated by "to limit the information (related to a specific key) available for cryptanalysis, limit exposure in the case of compromise of a single key; limit the use of a particular technology to its estimated effective lifetime; and limit the time available for computationally intensive cryptanalytic attacks" (e.g. page 553 of Menezes et al.)

As per **claims 2 and 13**, Asokan et al. – Menezes et al. discloses a method/system as applied in claims 1 and 12. Asokan et al. further discloses wherein

the first group key is generated using a group password of the ad-hoc group (P3, "choosing a fresh password and sharing it among those present in the room, P4 "In a landmark paper [4]....encrypted key exchange (EKE)...derive a strong and P5 "shared key starting from only a weak shared key")

As per **claims 3 and 14**, Asokan et al. – Menezes et al. discloses a method/system as applied in claims 1 and 12. Asokan et al. further discloses wherein the main wireless terminal encodes the second group key using the first group key, and transmits the encoded second group key to the (N-1) wireless terminals (P5, "In step 1 A sends E_a encrypted with the weak secret PAt this point, each player will compute the session key as $K=f(S_a, S_b)$ and P6, "One obvious way....and distribute it to the members of the group using the pairwise session keys he shares with them").

As per **claims 4 and 15**, Asokan et al. – Menezes et al. discloses a method/system as applied in claims 1 and 12. Asokan et al. further discloses wherein the main wireless terminal is a creator of the ad-hoc group (P 18, "for example,...the leader M_n has a greater say in the final session key...before finding one that leads to a particular type of K " and "In some ad-hoc networks there may already be a natural leader or ordering").

As per **claims 5 and 16**, Asokan et al. – Menezes et al. discloses a method/system as applied in claims 1 and 12. Asokan et al. further inherently discloses

wherein when the main wireless terminal is withdrawn from the ad-hoc group, the main wireless terminal transfers a function of key distribution center to a sub wireless terminal selected from among the (N-1) sub wireless terminals, so that the sub wireless terminal acts as the main wireless terminal (P16, "Therefore, when there is no a.priori leader or ordering...The general approach...This computation can be car- and P17, "ried out...to their distance from the reference value" and P20, "If groups are dynamic, the session key needs to updated when the composition of the group changes").

As per **claims 8 and 17-18**, Asokan et al. – Menezes et al. discloses a method/system as applied in claims 1 and 12. Asokan et al. further discloses:

if the first group key is created, encoding a second group key request message from one of the (N-1) sub wireless terminals, and transmitting the encoded second group key request message to the main wireless terminal (Page 5, "B extracts E_a , generates R randomly, encrypts it with E_a , and returns it to A in step 2");

decoding the second group key request message, using the first group key, in the main wireless terminal (P5, "The goal of the protocol is for A and B to mutually authenticate each other based on P , and to agree on a strong session key K ...each player will compute the session key as $K=f(S_a, S_b)$ "); and

creating a second group key according to the decoded second group key request message, in the main wireless terminal (P6, "an additional round...he shares with them").

As per **claim 9**, Asokan et al. – Menezes et al. discloses the claimed method of steps as applied above in claim 1. Therefore, Asokan et al. – Menezes et al. discloses a computer readable medium having embodied thereon the claimed computer program for carrying out the method of steps.

As per **claim 10**, Asokan et al. – Menezes et al. discloses the claimed method of steps as applied above in claim 3. Therefore, Asokan et al. – Menezes et al. discloses a computer readable medium having embodied thereon the claimed computer program for carrying out the method of steps.

As per **claim 11**, Asokan et al. – Menezes et al. discloses the claimed method of steps as applied above in claim 8. Therefore, Asokan et al. – Menezes et al. discloses a computer readable medium having embodied thereon the claimed computer program for carrying out the method of steps.

As per **claim 21 and 23**, they are rejected using the same rationale of rejecting claims 1 and 12 above.

As per **claims 24-25**, they are rejected using the same rationale of rejecting claims 1, 8, 12 and 17 above.

13. Claims 7, 20 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Asokan et al. – Menezes et al. as applied to claims 1-6, 8-10 and 11-19 and 21 above, further in view of Schneier ("Applied Cryptography" second edition, 1996)

As per **claims 7, 20 and 22**, the difference between the claimed invention and that disclosed in Asokan et al. – Menezes et al. is the latter does not disclose the claimed feature of the modified second group key is encoded using a non-modified second group key, and transmitting the encoded second group key to the (N-1) sub wireless terminals. However, such missing feature in Asokan et al. – Menezes et al. is clearly taught section 8.6 Updating keys on page 180, of the aforementioned Schneier reference, the same field endeavor of key management in the network environment. It would have been obvious for a person having ordinary skill in the art to incorporate such well known feature as taught in the Schneier reference into the Asokan et al. – Menezes et al. method motivated by to provide "an easier solution is to generate a new key from the old key" (Schneier, Section 8.6 on page 180)

14. Claims 1-5, 8-10 and 11-18, 21 and 23-25 are rejected under 35 U.S.C. 102(b) as being anticipated by Asokan et al. ("Key agreement in ad hoc networks", Computer Communications, Volume 23, Number 17, 1 November 2000) in view of Billhartz et al. (U.S. Pub. No. 20030210787).

As per **claims 1 and 12**, Asokan et al. discloses a cryptographic method/system using dual keys in a wireless local area network (LAN) system, comprising:

(a) generating a first group key ("At the end of the protocol run, each player shares a key with the leader" - e.g. page 6. Please note a key corresponds to Applicant's first group key) in N wireless terminals (forming an ad-hoc group (an ad-hoc meeting –e.g. p1, "They would like to set up a wireless network session...for the during

of the meeting”), where N is equal to or greater than two (P5, “There are two parties A and B which share a weak secret P” and P6 “We can slightly modify this....to a contributory multi-party protocol”) ;

(b) generating an initial second group key in a main wireless terminal (a leader – e.g. P6) to perform a key distribution center function among the N wireless terminals in response to a request from one of (N-1) sub wireless terminals (“The leader will broadcast the message in step 1...An additional round will be needed for the leader to pick a common session key and distribute it to the members of the group...he shares with them” – e.g. page 6. Please note on pages 5-6 of Asokan et al. reference, “In step 1 A sends Ea encrypted with the weak secret P...One obvious way to extend this protocol to the multi-party case is to elect a leader”, which met the claimed limitation of a request from one of (N-1) sub wireless terminals) the request being communicated using the first group key, and transmitting the initial second group key to (N-1) sub wireless terminals (P6, “An additional round will....to pick a common session key and distribute it the members of the group....he shares with them”. Asokan et al. also discloses on page 3, “1.3 Password-based Authenticated Key Exchange...by choosing a fresh password and sharing it among those present in the room...Therefore, we need a protocol to derive a strong shared session key from the weak shared password” – e.g. page 3. Please note a weak shared password corresponds to Applicant’s first group key and a strong shared session key corresponds to Applicant’s second group key. Asokan et al. further discloses on page 4, “The basic secrecy requirement is that only those players that know the initial password should learn the resulting session key,

which met the claimed limitation of the request being communicated using the first group key. In other words, the requesting member must prove his/her membership in the request by using the initial password (i.e. first group key); and

(c) encoding data using the initial second group key, and transmitting the encoded data between the N wireless terminals (P4 "In a landmark paper [4], Bellovin and Merrit....encrypted key exchange (EKE) and P5 "But the basic form of the generic protocol remains the same." Inherently, Asokan et al. teaches after the protocol is complete, the multi parties must communicate using the session key (the second group key) to encoding data and transmitting the encoded data among the N wireless terminals since the protocol is using encrypted key exchange (EKE), a well known protocol invented by Bellovin and Merrit disclosed on the P4 of the Asokan et al. reference).

(d) modifying the initial second group key in the main wireless terminal according to a modification time period, predetermined in the main wireless terminal, and transmitting the modified second group key to the (N-1) sub wireless terminals, wherein at least one modified second group key is transmitted and used to encode data during use of the first group key (P5, "session key"- a session key is a key that is just used for one communication session and then discarded, Page 20, "multi-party key agreement will need to address the issues of synchronization and resilience in face of benign faults... and page 11, "at the end of the round, all four players will have the same key...", "The time needed will be the same as that of one two-party key exchange" – page 12, "Synchronous rounds could be implemented if

all nodes have loosely synchronized clocks" – page 12, "...key exchange can be done efficiently, in terms of the number of communication rounds.." – page 10, "The protocol proceeds through d rounds, $1, \dots, d$." – page 11 and "...between themselves in $k-1$ rounds...In the end of those $k-1$ rounds each group will have a shared key. For all $2k$ members to agree on a single shared key in round k ...**The time needed will be the same as that of one two-party key exchange.** Notice in round 1...In round k ,...doing key exchange in parallel" – page 12). Asokan et al. implicitly discloses modifying the initial second group key in the main wireless terminal according to a modification time period, predetermined in the main wireless terminal and transmitting the modified second group key to the $(N-1)$ sub wireless terminals, wherein at least one modified second group key is transmitted and used to encode data during use of the first group key since to an ordinary skill in the art that a session key in the Asokan et al. reference is for a fixed periods (i.e. session) and then need to be replaced and the password (i.e. first group key) is always present to verify membership for broadcasting a new session key the same way as the initial session key (i.e. initial second group key) is transmitted.

In order to make the record clearer, Billhartz et al. expressly discloses modifying the initial second group key in the main wireless terminal according to a modification time period, predetermined in the main wireless terminal ("Of course, the secret key may be periodically (e.g. daily, monthly, etc.) changed in some embodiments, if even

further security enhancements are desired..." – e.g. lines 5-7 of par. [0043] and please also note secret key in the Billhartz et al. reference is "shared between wireless stations ...The secret key is used to encrypt data packets..." in par. [0026]).

It would have been obvious to a person with ordinary skill in the art at the time of the invention to incorporate Billhartz et al.'s modifying the initial second group key in the main wireless terminal according to a modification time period, predetermined in the main wireless terminal into Asokan et al. motivated by "further security enhancements are desired, as will be appreciated by those skill in the art", as disclosed by Billhartz et al. (e.g. lines 6-7 of Billhartz et al.)

As per **claims 2 and 13**, Asokan et al. – Billhartz et al. discloses a method/system as applied in claims 1 and 12. Asokan et al. further discloses wherein the first group key is generated using a group password of the ad-hoc group (P3, "choosing a fresh password and sharing it among those present in the room, P4 "In a landmark paper [4]....encrypted key exchange (EKE)...derive a strong and P5 "shared key starting from only a weak shared key")

As per **claims 3 and 14**, Asokan et al. – Billhartz et al. discloses a method/system as applied in claims 1 and 12. Asokan et al. further discloses wherein the main wireless terminal encodes the second group key using the first group key, and transmits the encoded second group key to the (N-1) wireless terminals (P5, "In step 1 A sends Ea encrypted with the weak secret P....At this point, each player will compute

the session key as $K=f(S_a, S_b)$ and P6, "One obvious way....and distribute it to the members of the group using the pairwise session keys he shares with them").

As per **claims 4 and 15**, Asokan et al. – Billhartz et al. discloses a method/system as applied in claims 1 and 12. Asokan et al. further discloses wherein the main wireless terminal is a creator of the ad-hoc group (P 18, "for example,...the leader Mn has a greater say in the final session key...before finding one that leads to a particular type of K" and "In some ad-hoc networks there may already be a natural leader or ordering").

As per **claims 5 and 16**, Asokan et al. – Billhartz et al. discloses a method/system as applied in claims 1 and 12. Asokan et al. further inherently discloses wherein when the main wireless terminal is withdrawn from the ad-hoc group, the main wireless terminal transfers a function of key distribution center to a sub wireless terminal selected from among the (N-1) sub wireless terminals, so that the sub wireless terminal acts as the main wireless terminal (P16, "Therefore, when there is no a.priori leader or ordering...The general approach...This computation can be car- and P17, "ried out...to their distance from the reference value" and P20, "If groups are dynamic, the session key needs to updated when the composition of the group changes").

As per **claims 8 and 17-18**, Asokan et al. – Billhartz et al. discloses a method/system as applied in claims 1 and 12. Asokan et al. further discloses:

if the first group key is created, encoding a second group key request message from one of the (N-1) sub wireless terminals, and transmitting the encoded second group key request message to the main wireless terminal (Page 5, "B extracts E_a , generates R randomly, encrypts it with E_a , and returns it to A in step 2");

decoding the second group key request message, using the first group key, in the main wireless terminal (P5, "The goal of the protocol is for A and B to mutually authenticate each other based on P , and to agree on a strong session key K ...each player will compute the session key as $K=f(S_a, S_b)$ "); and

creating a second group key according to the decoded second group key request message, in the main wireless terminal (P6, "an additional round...he shares with them").

As per **claim 9**, Asokan et al. – Billhartz et al. discloses the claimed method of steps as applied above in claim 1. Therefore, Asokan et al. discloses a computer readable medium having embodied thereon the claimed computer program for carrying out the method of steps.

As per **claim 10**, Asokan et al. – Billhartz et al. discloses the claimed method of steps as applied above in claim 3. Therefore, Asokan et al. discloses a computer readable medium having embodied thereon the claimed computer program for carrying out the method of steps.

As per **claim 11**, Asokan et al. – Billhartz et al. discloses the claimed method of steps as applied above in claim 8. Therefore, Asokan et al. discloses a computer

readable medium having embodied thereon the claimed computer program for carrying out the method of steps.

As per **claim 21 and 23**, they are rejected using the same rationale of rejecting claims 1 and 12 above.

As per **claims 24-25**, they are rejected using the same rationale of rejecting claims 1, 8, 12 and 17 above.

15. Claims 7, 20 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Asokan et al. – Billhartz et al. as applied to claims 1-6, 8-10 and 11-19 and 21 above, further in view of Schneier ("Applied Cryptography" second edition, 1996)

As per **claims 7, 20 and 22**, the difference between the claimed invention and that disclosed in Asokan et al. – Billhartz et al. is the latter does not disclose the claimed feature of the modified second group key is encoded using a non-modified second group key, and transmitting the encoded second group key to the (N-1) sub wireless terminals. However, such missing feature in Asokan et al. – Billhartz et al. is clearly taught section 8.6 Updating keys on page 180, of the aforementioned Schneier reference, the same field endeavor of key management in the network environment. It would have been obvious for a person having ordinary skill in the art to incorporate such well known feature as taught in the Schneier reference into the Asokan et al. – Billhartz et al. method motivated by to provide "an easier solution is to generate a new key from the old key" (Schneier, Section 8.6 on page 180)

16. Claims 1-5, 8-10 and 11-18, 21 and 23-25 are rejected under 35 U.S.C. 102(b) as being anticipated by Asokan et al. ("Key agreement in ad hoc networks", Computer Communications, Volume 23, Number 17, 1 November 2000) in view of Kung et al. (U.S. Patent No. 6,889,321).

As per **claims 1 and 12**, Asokan et al. discloses a cryptographic method/system using dual keys in a wireless local area network (LAN) system, comprising:

(a) generating a first group key ("At the end of the protocol run, each player shares a key with the leader" - e.g. page 6. Please note a key corresponds to Applicant's first group key) in N wireless terminals (forming an ad-hoc group (an ad-hoc meeting -e.g. p1, "They would like to set up a wireless network session...for the during of the meeting"), where N is equal to or greater than two (P5, "There are two parties A and B which share a weak secret P" and P6 "We can slightly modify this....to a contributory multi-party protocol") ;

(b) generating an initial second group key in a main wireless terminal (a leader - e.g. P6) to perform a key distribution center function among the N wireless terminals in response to a request from one of (N-1) sub wireless terminals ("The leader will broadcast the message in step 1...An additional round will be needed for the leader to pick a common session key and distribute it to the members of the group...he shares with them" - e.g. page 6. Please note on pages 5-6 of Asokan et al. reference, "In step 1 A sends Ea encrypted with the weak secret P...One obvious way to extend this protocol to the multi-party case is to elect a leader", which met the claimed limitation of

a request from one of (N-1) sub wireless terminals) the request being communicated using the first group key, and transmitting the initial second group key to (N-1) sub wireless terminals (P6, "An additional round will...to pick a common session key and distribute it the members of the group....he shares with them". Asokan et al. also discloses on page 3, "1.3 Password-based Authenticated Key Exchange...by choosing a fresh password and sharing it among those present in the room...Therefore, we need a protocol to derive a strong shared session key from the weak shared password" – e.g. page 3. Please note a weak shared password corresponds to Applicant's first group key and a strong shared session key corresponds to Applicant's second group key. Asokan et al. further discloses on page 4, "The basic secrecy requirement is that only those players that know the initial password should learn the resulting session key, which met the claimed limitation of the request being communicated using the first group key. In other words, the requesting member must prove his/her membership in the request by using the initial password (i.e. first group key); and

(c) encoding data using the initial second group key, and transmitting the encoded data between the N wireless terminals (P4 "In a landmark paper [4], Bellare and Merritt....encrypted key exchange (EKE) and P5 "But the basic form of the generic protocol remains the same." Inherently, Asokan et al. teaches after the protocol is complete, the multi parties must communicate using the session key (the second group key) to encoding data and transmitting the encoded data among the N wireless terminals since the protocol is using encrypted key exchange (EKE), a well known

protocol invented by Bellovin and Merrit disclosed on the P4 of the Asokan et al. reference).

(d) modifying the initial second group key in the main wireless terminal according to a modification time period, predetermined in the main wireless terminal, and transmitting the modified second group key to the (N-1) sub wireless terminals, wherein at least one modified second group key is transmitted and used to encode data during use of the first group key (P5, "session key"- a session key is a key that is just used for one communication session and then discarded, Page 20, "multi-party key agreement will need to address the issues of synchronization and resilience in face of benign faults... and page 11, "at the end of the round, all four players will have the same key...", "The time needed will be the same as that of one two-party key exchange" – page 12, "Synchronous rounds could be implemented if all nodes have loosely synchronized clocks" – page 12, "...key exchange can be done efficiently, in terms of the number of communication rounds.." – page 10, "The protocol proceeds through d rounds, 1,..., d." – page 11 and "...between themselves in k-1 rounds...In the end of those k-1 rounds each group will have a shared key. For all 2k members to agree on a single shared key in round k...**The time needed will be the same as that of one tow-party key exchange.** Notice in round 1...In round k,...doing key exchange in parallel" – page 12). Asokan et al. implicitly discloses modifying the initial second group key in the main wireless terminal according to a modification time period, predetermined in the main wireless terminal and transmitting the modified second group key to the (N-1) sub wireless terminals,

wherein at least one modified second group key is transmitted and used to encode data during use of the first group key since to an ordinary skill in the art that a session key in the Asokan et al. reference is for a fixed periods (i.e. session) and then need to be replaced and the password (i.e. first group key) is always present to verify membership for broadcasting a new session key the same way as the initial session key (i.e. initial second group key) is transmitted.

In order to make the record clearer, Kung et al. expressly discloses modifying the initial second group key in the main wireless terminal according to a modification time period, predetermined in the main wireless terminal ("...As such, the encryption key...may be **repeatedly updated and changed at various time intervals. The repeated updates may be at periodic (e.g., daily)...**" – e.g. col. 34, lines 25-46 and col. 2,, lines 46-58 of Kung et al.).

It would have been obvious to a person with ordinary skill in the art at the time of the invention to incorporate Kung et al.'s modifying the initial second group key in the main wireless terminal according to a modification time period, predetermined in the main wireless terminal into Asokan et al. motivated by to enhance security in data communication so that a hacker that breaks an encryption key at any point in time will not have continuous communication security intrusion (e.g. Kung et al. col. 2, lines 46-54).

As per **claims 2 and 13**, Asokan et al. – Kung et al. discloses a method/system as applied in claims 1 and 12. Asokan et al. further discloses wherein the first group key is generated using a group password of the ad-hoc group (P3, “choosing a fresh password and sharing it among those present in the room, P4 “In a landmark paper [4]...encrypted key exchange (EKE)...derive a strong and P5 “shared key starting from only a weak shared key”)

As per **claims 3 and 14**, Asokan et al. – Kung et al. discloses a method/system as applied in claims 1 and 12. Asokan et al. further discloses wherein the main wireless terminal encodes the second group key using the first group key, and transmits the encoded second group key to the (N-1) wireless terminals (P5, “In step 1 A sends E_a encrypted with the weak secret PAt this point, each player will compute the session key as $K=f(S_a, S_b)$ and P6, “One obvious way....and distribute it to the members of the group using the pairwise session keys he shares with them”) .

As per **claims 4 and 15**, Asokan et al. – Kung et al. discloses a method/system as applied in claims 1 and 12. Asokan et al. further discloses wherein the main wireless terminal is a creator of the ad-hoc group (P 18, “for example,...the leader M_n has a greater say in the final session key...before finding one that leads to a particular type of K ” and “In some ad-hoc networks there may already be a natural leader or ordering”).

As per **claims 5 and 16**, Asokan et al. – Kung et al. discloses a method/system as applied in claims 1 and 12. Asokan et al. further inherently discloses wherein when the main wireless terminal is withdrawn from the ad-hoc group, the main wireless terminal transfers a function of key distribution center to a sub wireless terminal selected from among the (N-1) sub wireless terminals, so that the sub wireless terminal acts as the main wireless terminal (P16, "Therefore, when there is no a.priori leader or ordering...The general approach...This computation can be car- and P17, "ried out...to their distance from the reference value" and P20, "If groups are dynamic, the session key needs to updated when the composition of the group changes").

As per **claims 8 and 17-18**, Asokan et al. – Kung et al. discloses a method/system as applied in claims 1 and 12. Asokan et al. further discloses:

if the first group key is created, encoding a second group key request message from one of the (N-1) sub wireless terminals, and transmitting the encoded second group key request message to the main wireless terminal (Page 5, "B extracts E_a , generates R randomly, encrypts it with E_a , and returns it to A in step 2");

decoding the second group key request message, using the first group key, in the main wireless terminal (P5, "The goal of the protocol is for A and B to mutually authenticate each other based on P , and to agree on a strong session key K ...each player will compute the session key as $K=f(S_a, S_b)$ "); and

creating a second group key according to the decoded second group key request message, in the main wireless terminal (P6, "an additional round...he shares with them").

As per **claim 9**, Asokan et al. – Kung et al. discloses the claimed method of steps as applied above in claim 1. Therefore, Asokan et al. discloses a computer readable medium having embodied thereon the claimed computer program for carrying out the method of steps.

As per **claim 10**, Asokan et al. – Kung et al. discloses the claimed method of steps as applied above in claim 3. Therefore, Asokan et al. discloses a computer readable medium having embodied thereon the claimed computer program for carrying out the method of steps.

As per **claim 11**, Asokan et al. – Kung et al. discloses the claimed method of steps as applied above in claim 8. Therefore, Asokan et al. discloses a computer readable medium having embodied thereon the claimed computer program for carrying out the method of steps.

As per **claim 21 and 23**, they are rejected using the same rationale of rejecting claims 1 and 12 above.

As per **claims 24-25**, they are rejected using the same rationale of rejecting claims 1, 8, 12 and 17 above.

17. Claims 7, 20 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Asokan et al. – Kung et al. as applied to claims 1-6, 8-10 and 11-19 and 21 above, further in view of Schneier ("Applied Cryptography" second edition, 1996)

As per **claims 7, 20 and 22**, the difference between the claimed invention and that disclosed in Asokan et al. – Kung et al. is the latter does not disclose the claimed feature of the modified second group key is encoded using a non-modified second group key, and transmitting the encoded second group key to the (N-1) sub wireless terminals. However, such missing feature in Asokan et al. – Kung et al. is clearly taught section 8.6 Updating keys on page 180, of the aforementioned Schneier reference, the same field endeavor of key management in the network environment. It would have been obvious for a person having ordinary skill in the art to incorporate such well known feature as taught in the Schneier reference into the Asokan et al. – Kung et al. method motivated by to provide "an easier solution is to generate a new key from the old key" (Schneier, Section 8.6 on page 180).

Conclusion

18. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. (See PTO-892).

The Applicant is strongly urged to review all the references cited by the examiner in response to the current Office Action.

Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to APRIL Y. SHAN whose telephone number is (571)270-

1014. The examiner can normally be reached on Monday - Friday, 8:00 a.m. - 5:00 p.m., EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/April Y Shan/
Examiner, Art Unit 2135

/KimYen Vu/

Supervisory Patent Examiner, Art Unit 2135